Department of Justice
U.S. Attorney's Office
Northern District of California

FOR IMMEDIATE RELEASE Friday, July 31, 2020

Three Individuals Charged For Alleged Roles In Twitter Hack

SAN FRANCISCO– Three individuals have been charged today for their alleged roles in the Twitter hack that occurred on July 15, 2020.

The announcement was made by United States Attorney David L. Anderson; Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division; FBI Special Agent in Charge John L. Bennett; Kelly R. Jackson, IRS Criminal Investigation, Special Agent in Charge of the Washington D.C. Field Office; U.S. Secret Service Special Agent in Charge of the San Francisco Field Office Thomas Edwards and U.S. Secret Service Special Agent in Charge of the Orlando Field Office Caroline O'Brien Buster. Additional facts regarding the investigation and charges can be found here: https://youtu.be/z80K3-q3Kqg.

Mason Sheppard, aka "Chaewon," 19, of Bognor Regis, in the United Kingdom, was charged in a criminal complaint in the Northern District of California with conspiracy to commit wire fraud, conspiracy to commit money laundering, and the intentional access of a protected computer.

Nima Fazeli, aka "Rolex," 22, of Orlando, Florida, was charged in a criminal complaint in the Northern District of California with aiding and abetting the intentional access of a protected computer.

The third defendant is a juvenile. With exceptions that do not apply to this case, juvenile proceedings in federal court are sealed to protect the identity of the juvenile. Pursuant to the Federal Juvenile Delinquency Act, the Justice Department has referred the individual to the State Attorney for the 13th Judicial District in Tampa, Florida.

"There is a false belief within the criminal hacker community that attacks like the Twitter hack can be perpetrated anonymously and without consequence," said U.S. Attorney David L. Anderson for the Northern District of California. "Today's charging announcement demonstrates that the elation of nefarious hacking into a secure environment for fun or profit will be short-lived. Criminal conduct over the Internet may feel stealthy to the people who perpetrate it, but there is nothing stealthy about it. In particular, I want to say to would-be offenders, break the law, and we will find you."

"The hackers allegedly compromised over 100 social media accounts and scammed both the account users and others who sent money based on their fraudulent solicitations," said Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division. "The rapid investigation of this conduct is a testament to the expertise of our investigators, our commitment to responding quickly to cyber attacks, and the close relationships we have built with law enforcement partners throughout the world."

"Upon opening an investigation into this attack, our investigators worked quickly to determine who was responsible and to locate those individuals," said San Francisco FBI Special Agent in Charge John F. Bennett. "While investigations into cyber breaches can sometimes take years, our investigators were able to bring these hackers into custody in a matter of weeks. Regardless of how long it takes us to identify hackers, we will follow the evidence to where it leads us and ultimately hold those responsible for cyber intrusions accountable for their actions. Cyber criminals will not find sanctuary behind their keyboards."

"Weeks ago, one of the world's most prolific social media platforms came under attack. Various political leaders, celebrities, and influencers were virtually held hostage as their accounts were hacked," said Kelly R. Jackson, IRS-Criminal Investigation (IRS-CI) Special Agent in Charge of the Washington D.C. Field Office. "The public was confused, and everyone wanted answers. We can now start answering those questions thanks to the work of IRS-CI cyber-crime experts and our law enforcement partners. Washington DC Field Office Cyber Crimes Unit analyzed the blockchain and de-anonymized bitcoin transactions allowing for the identification of two different hackers. This case serves as a great example of how following the money, international collaboration, and public-private partnerships can work to successfully take down a perceived anonymous criminal enterprise. Regardless of the illicit scheme, and whether the proceeds are virtual or tangible, IRS-CI will continue to follow the money and unravel complex financial transactions."

"Today's announcement proves that cybercriminals can no longer hide behind perceived global anonymity," said Thomas Edwards, Special Agent in Charge, U.S. Secret Service, San Francisco Field Office. "The Secret Service remains committed to pursuing those responsible for cyber-enabled fraud and will continue to hold cyber criminals accountable for their actions. This investigation is a testament to the strong partnerships between the Secret Service, the U.S. Attorney's Office, the FBI, the IRS, as well as our state, local and international law enforcement partners."

"Our identities and reputations are sacred. We will continue to aggressively defend and protect individuals, companies, and other entities from new-age cyber-fraud, especially those who scheme to hack, defraud and wreak havoc on U.S. citizens across the country," said Caroline O'Brien Buster, Special Agent in Charge, U.S. Secret Service, Orlando Field Office. "The Secret Service believes that building trusted partnerships between the private sector and all levels of law enforcement is the proven model for success. I commend the exceptional work conducted by our law enforcement partners and the U.S. Attorney's Office who worked diligently to hold these defendants accountable."

As alleged in the complaints, the Twitter attack consisted of a combination of technical breaches and social engineering. The result of the Twitter hack was the compromise of approximately 130 Twitter accounts pertaining to politicians, celebrities, and musicians.

The hackers are alleged to have created a scam bitcoin account, to have hacked into Twitter VIP accounts, to have sent solicitations from the Twitter VIP accounts with a false promise to double any bitcoin deposits made to the scam account, and then to have stolen the bitcoin that victims

deposited into the scam account. As alleged in the complaints, the scam bitcoin account received more than 400 transfers worth more than $100,000.

This case is being investigated by the FBI's San Francisco Division, with assistance from the IRS-Criminal Investigation Cyber Unit; the U.S. Secret Service, San Francisco and Headquarters; the Santa Clara County Sheriff's Office and their REACT task force and the Florida Department of Law Enforcement.

The case is being prosecuted by Assistant U.S. Attorneys William Frentzen and Andrew Dawson of the Northern District of California and Senior Counsel Adrienne Rose of the Criminal Division's Computer Crime and Intellectual Property Section.

Additional assistance has been provided by the U.S. Attorney's Office for the Middle District of Florida; the State Attorney for the 13th Judicial District in Tampa, Florida; the Criminal Division's Office of International Affairs and Organized Crime and Gang Section; the United Kingdom's Central Authority and National Crime Agency; Chainalysis and Excygent.

The allegations of a criminal complaint are merely allegations, and the defendants are presumed innocent unless or until the allegations against them are proved beyond any reasonable doubt.